

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Бублик Владимир Александрович
Должность: Ректор
Дата подписания: 28.08.2023 10:49:09
Уникальный программный ключ:
c51e862f35fca08ce36bdc9169348d2ba451f033

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
Федеральное государственное бюджетное образовательное
учреждение высшего образования
**«УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ
ИМЕНИ В.Ф. ЯКОВЛЕВА»**

«Утверждено»
Решением Ученого Совета УрГЮУ
имени В.Ф. Яковлева
от «26» июня 2023 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Правовое регулирование информационной безопасности»
Основная профессиональная образовательная программа высшего
образования – программа магистратуры по направлению подготовки
40.04.01 Юриспруденция
(профиль (магистерская программа): Правовое обеспечение экономической деятельности
и цифровой экономики)

РАЗРАБОТЧИК	
КАФЕДРА:	Информационного права
АВТОР (Ы):	Паршуков Михаил Игоревич, к.ю.н., доцент

Целью освоения учебной дисциплины является формирование у студентов современных углубленных знаний, практических умений и навыков в области обеспечения информационной безопасности, в т.ч. правовой защиты государственной тайны, служебной тайны, коммерческой тайны, профессиональных тайн, персональных данных. В рамках изучения дисциплины дается комплексный подход к обеспечению информационной безопасности с учетом использования современных информационных технологий и средств; рассматриваются прикладные вопросы защиты информации.

Дисциплина относится к части учебного плана, формируемой участниками образовательных отношений.

ТЕМАТИЧЕСКИЙ ПЛАН

№ п/п	Темы учебной дисциплины	Виды учебной деятельности и трудоемкость (в часах)			Всего часов
		Лекции	Практические занятия	Самостоятельная работа	
I	Модуль 1. Основы теории информационной безопасности				
1	Тема 1. Понятие и система информационной безопасности. Угрозы информационной безопасности. Государственная политика в области обеспечения информационной безопасности.	1	1	6	8
2	Тема 2. Организационное обеспечение информационной безопасности	1	1	6	8
3	Тема 3. Правовое обеспечение информационной безопасности	2	2	6	10
4	Тема 4. Технические средства обеспечения информационной безопасности	1	1	6	8
5	Тема 5. Технологические средства обеспечения информационной безопасности	1	1	6	8
II	Модуль 2. Правовой режим информации ограниченного доступа.				
6	Тема 6. Тайна как правовая категория. Общий правовой режим информации ограниченного доступа.	1	1	6	8

7	Тема 7. Правовой режим государственной тайны.	1	1	6	8
8	Тема 8. Правовой режим служебной тайны. Служебная тайна в области обороны. Служебная информация ограниченного распространения в федеральных органах государственной власти.	2	1	6	9
9	Тема 9. Правовой режим коммерческой тайны. Понятие и признаки коммерческой тайны. Правовой режим коммерческой тайны. Группы сведений, составляющих коммерческую тайну. Субъекты коммерческой тайны. Условия передачи сведений, составляющих коммерческую тайну третьим лицам.	2	2	7	10
10	Тема 10. Правовой режим персональных данных.	2	2	7	11
11	Тема 11. Информационные правонарушения. Понятие и система информационных правонарушений. Административные информационные правонарушения. Понятие и виды. Дисциплинарные информационные правонарушения. Понятие и виды. Гражданско-правовые информационные правонарушения. Понятие и виды. Понятие и виды информационных преступлений. Проблемы предупреждения информационных правонарушений.	1	2	7	10
12	Тема 12. Информационное противоборство	1	1	7	10
ВСЕГО:		16	16	76	108

РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ:

Типы задач профессиональной деятельности	Задачи профессиональной деятельности	Код профессиональной компетенции	Содержание профессиональной компетенции	Код индикатора	Содержание индикатора	Результаты обучения
правоприменительный	Правовое сопровождение деятельности хозяйствующих субъектов, в том числе деятельности, осуществляемой с помощью электронных или цифровых технологий	ПК-5	Способен обеспечивать соблюдение законности в деятельности хозяйствующего субъекта и защиту его правовых интересов	ИПК-5.1	Организует подготовку документов, регламентирующих организационно-правовые вопросы уставной деятельности организации, локальных нормативных актов, связанных с осуществлением службами (работниками) своих функций, локальных нормативных актов, регулирующих трудовые правоотношения, и иных документов правового характера	Знания: Организация информационной безопасности. Директивные документы по обеспечению информационной безопасности. Кадровое обеспечение информационной безопасности. Умения: анализировать правовые нормы об обеспечении государственной политики в области информатики и информационной безопасности. Навыки: создания локальных нормативных актов по вопросам защиты коммерческой тайны и персональных данных
				ИПК-5.4	Организует правовое сопровождение деятельности иных структурных	Умения: определять допустимые нормативно-правовыми актами виды технических и

					<p>подразделений (работников), связанной с осуществлением ими своих функций (кадровой службой, службой экономической безопасности, бухгалтерской службой и пр.)</p>	<p>технологических средств обеспечения информационной безопасности, описывать в локальных нормативных актах инженерно-технические, методические, криптографические и программно-аппаратные способы обеспечения информационной безопасности.</p> <p>Навыки: создания локальных нормативных актов в сфере информационной безопасности. Применения правовых норм в области обеспечения информационной безопасности.</p>
				ИПК-5.6	<p>Обеспечивает правовую охрану и защиту прав на результаты интеллектуальной деятельности и средства индивидуализации</p>	<p>Знания: Режим защиты коммерческой тайны. Понятие и природа коммерческой тайны. Нормативное закрепление правового режима коммерческой тайны. Методическое обеспечение определения сведений, составляющей коммерческую тайну. Субъекты коммерческой тайны. Условия передачи информации, составляющей коммерческую тайну.</p> <p>Умения: Совершать юридически значимые</p>

						<p>действия в области информации ограниченного доступа. Анализировать нормы правовых актов в области информации ограниченного доступа</p> <p>Навыки: создания локальных нормативных актов в области обеспечения защиты коммерческой тайны. Навыки предупреждения опасностей и угроз, возникающих в информационных процессах</p>
		ПК-6	Способен обеспечивать правовое сопровождение цифровой трансформации деятельности хозяйствующего субъекта	ИПК-6.1	Организует и осуществляет правовое сопровождение деятельности хозяйствующих субъектов по внедрению, масштабированию и использованию электронных и цифровых технологий в экономической деятельности	<p>Знания: Информация юридических лиц и ее место в информационном обществе. Особенности и порядок защиты информации в корпорациях. Кадровое обеспечение в организациях в области защиты информации. Управление рисками в области защиты информации.</p> <p>Умения: Давать квалифицированные юридические заключения, проводить консультации по вопросам обеспечения информационной безопасности.</p> <p>Навыки: использования современных информационных технологий и баз данных (в частности баз</p>

						данных ФСТЭК по информационным угрозам) для функционирования организации
Представление интересов субъекта экономической деятельности	ПК-7	Способен представлять интересы субъекта экономической деятельности в суде, арбитражном суде, осуществлять ведение судебных и арбитражных дел	ИПК-7.1	Осуществляет руководство и принимает участие в подготовке и оформлении различного рода правовых документов в рамках гражданского и административного судопроизводства в интересах представляемого лица	Знания: Базовые законы в сфере информационной безопасности. Подзаконные акты в сфере информационной безопасности. Локальные нормативные акты в сфере информационной безопасности. Стандарты и регламенты. Международные стандарты в сфере информационной безопасности. Умения: анализировать правовые нормы об обеспечении государственной политики в области информатики и информационной безопасности Навыки: Выявления обстоятельств, способствующих совершению информационных правонарушений	
			ИПК-7.2	Руководит и принимает участие в осуществлении от имени и в интересах представляемого лица полномочий и всех процессуальных	Знания: Понятие и система информационных преступлений. Классификация информационных преступлений. Проблемы предупреждения	

					<p>действий, предоставляемых стороне во всех судах и во всех инстанциях суда общей юрисдикции</p>	<p>информационных преступлений. Международные проблемы борьбы с информационными преступлениями</p> <p>Умения: Правильно применять современные информационные технологии для оформления юридических документов в области информационной безопасности. Совершать юридически значимые действия в области управления рисками в информационной безопасности. Осуществлять поиск информации о лицензировании и аттестации в области защиты информации</p>
				ИПК-7.3	<p>Руководит и принимает участие в осуществлении от имени и в интересах представляемых лиц полномочий и всех процессуальных действий, предоставляемых стороне во всех судах и во всех инстанциях арбитражного суда</p>	<p>Знания: Режим защиты персональных данных. Персональные данные как форма защиты частной жизни. Система законодательства о защите персональных данных. Условия работы с персональными данными. Методическое обеспечение защиты персональных данных. Ответственность за нарушения порядка обработки персональных данных</p> <p>Умения: Правильно</p>

						применять современные информационные технологии для оформления юридических документов в области информационной безопасности. Совершать юридически значимые действия в области управления рисками в информационной безопасности. Осуществлять поиск информации о лицензировании и аттестации в области защиты информации
		ПК-8	Способен представлять интересы субъекта экономической деятельности в государственных и общественных организациях при рассмотрении правовых вопросов	ИПК-8.1	Осуществляет руководство и принимает участие в подготовке и оформлении различного рода правовых документов для органов государственной власти, органов местного самоуправления, общественных объединений и иных организаций в интересах представляемого лица	Знания: Режим защиты государственной тайны. Государственная тайна как особый вид информации ограниченного доступа. Перечень сведений, составляющих государственную тайну. Условия допуска к государственной тайне. Порядок защиты государственной тайны. Ответственность за нарушение режима государственной тайны. Умения: Осуществлять обеспечение защиты государственной тайны. Совершать юридически значимые действия в области

						информации ограниченного доступа. Анализировать нормы правовых актов в области тайн.
				ИПК-8.2	Осуществляет руководство и принимает участие во взаимодействии от имени и в интересах представляемых лиц с органами государственной власти, органами местного самоуправления, общественными объединениями и иными организациями при рассмотрении правовых вопросов	Знания: Режим защиты служебной тайны. Понятие служебной тайны. Нормативное закрепление правового режима служебной тайны. Порядок работы с информацией, составляющей служебную тайну Умения: Осуществлять обеспечение защиты служебной тайны. Совершать юридически значимые действия в области информации ограниченного доступа. Анализировать нормы правовых актов в области тайн.
экспертно-аналитический	Правовой анализ	ПК-11	Способен составлять юридические заключения по правовым вопросам	ИПК-11.1	Осуществляет руководство и принимает участие в подготовке юридических заключений по вопросам деятельности хозяйствующего субъекта, в том числе на основе применения современных информационных технологий и вычислительных средств	Знания: Понятие защиты информации. Концепция комплексной системы защиты информации. Модель защиты информации. Классификация уровней защищенности информации. Практические проблемы реализации комплексной системы защиты информации. Понятие системы лицензирования в области защиты информации. Аттестация объектов

						информатизации по требованиям безопасности информации. Сертификация продукции и услуг в области защиты информации. Система органов по сертификации средств защиты информации. Ответственность в области защиты информации.
консультационный	Консультирование по правовым вопросам	ПК-12	Способен организовывать и осуществлять консультирование по правовым вопросам	ИПК-12.3	Консультирует на предмет существования правовых рисков и возможных ограничений при внедрении цифровых технологий в экономическую деятельность субъекта	Знания: Понятие и виды технических средств обеспечения информационной безопасности. Методическое обеспечение информационной безопасности. Криптографические методы обеспечения информационной безопасности. Программно-аппаратное обеспечение информационной безопасности.
организационно-управленческой	Организационное обеспечение деятельности	ПК-13	Способен осуществлять организационное обеспечение деятельности хозяйствующего субъекта	ИПК-13.2	Организует взаимодействие юридических служб или самостоятельно взаимодействует со специалистами в области информационных технологий при создании баз данных, размещении на сайте компании информации о последних обновлениях в законодательстве,	Знания: понятие и систему информационной безопасности. Угрозы информационной безопасности понятие защищенности интересов личности, общества и государства в информационной сфере. Классификацию национальных интересов в области информационной безопасности. Понятие

					<p>раскрытии информации, обязательной для субъекта экономической деятельности</p>	<p>системы обеспечения информационной безопасности. Силы и средства обеспечения информационной безопасности. Технические и технологические средства обеспечения информационной безопасности. Понятие угроз информационной безопасности. Угрозы интересам личности в информационной сфере. Угрозы интересам общества в информационной сфере. Угрозы интересам государства в информационной сфере. Понятие информационных войн в системе угроз информационной безопасности.</p> <p>Умения: получать новые и применять полученные знания в практической деятельности по укреплению законности и правопорядка в сфере информационной безопасности. Определять юридическую природу и характер информационных правоотношений, отличать их от смежных отношений.</p> <p>Навыки: совершенствования профессиональных знаний и</p>
--	--	--	--	--	---	--

						профессионального опыта в сфере правового обеспечения информационной безопасности
--	--	--	--	--	--	--

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Использование технологий

- для проведения видеоконференций: GoogleMeet, Яндекс.Телемост, Zoom
- для проведения текущего контроля, фиксации активности изучения Moodle
- фиксация и отслеживание текущей активности (во время занятия) Mentimetr
- получение правовой информации: СПС Консультант, СПС Кодекс, СПС Гарант
- получение официальной информации: портал Официальная Россия, портал Госуслуги, ГАС «Правосудие», ИС «Мой арбитр», ГАС «Правовая статистика».
- он-лайн обучение (для дистанта) Moodle, Он-лайн офис Google, Яндекс.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 1. Входной контроль. Понятие и система информационной безопасности. Угрозы информационной безопасности. Государственная политика в области обеспечения информационной безопасности.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 2. Правовое обеспечение информационной безопасности

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 3. Технические средства обеспечения информационной безопасности. Технологическое обеспечение информационной безопасности

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 4. Тайна как правовая категория. Общий правовой режим информации ограниченного доступа.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 5. Правовой режим государственной тайны. Правовой режим служебной тайны. Служебная тайна в области обороны. Служебная информация ограниченного распространения в федеральных органах государственной власти.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 6. Правовой режим коммерческой тайны. Понятие и признаки коммерческой тайны. Правовой режим коммерческой тайны. Группы сведений, составляющих коммерческую тайну. Субъекты коммерческой тайны. Условия передачи сведений, составляющих коммерческую тайну третьим лицам.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 7. Правовой режим персональных данных.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ 8. Информационные правонарушения. Понятие и система информационных правонарушений. Административные информационные правонарушения: понятие и виды.

Дисциплинарные информационные правонарушения: понятие и виды. Гражданско-правовые информационные правонарушения: понятие и виды. Понятие и виды информационных преступлений. Проблемы предупреждения информационных правонарушений. Информационное противоборство.

РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Занятия по дисциплине проводятся в виде лекционных, практических и самостоятельных занятий.

Тема практического занятия в соответствии с тематическим планом озвучивается преподавателем студентам на предыдущем практическом занятии и размещается материалы на учебном портале Университета. К практическому занятию студентам в обязательном порядке необходимо ознакомиться с текстом нормативно-правовых актов,

учебной и научной литературой по указанной теме (список литературы и НПА на учебном портале Moodle, в РПД). Практическое занятие проходит в форме диалога, который определяет уровень теоретической подготовки студента; решения практических задач с использованием сети интернет и справочных правовых систем, что позволяет оценить уровень знаний, умений и владений студента по указанной теме.

ТЕКУЩИЙ КОНТРОЛЬ

Задания для практической части семинарского занятия озвучиваются преподавателем на семинаре.

Задания для самостоятельной работы студента по теме озвучиваются преподавателем на семинаре.

Ссылки на тексты рекомендуемых к изучению научных работ (статей ученых) размещаются на учебном портале.

Форма контроля по теме – устный опрос, выполнение практических заданий.

Система оценивания по дисциплине:

Перечень тем/модулей, по которым проводится контрольное мероприятие	Форма и описание контрольного мероприятия	Балловая стоимость контрольного мероприятия и критерии начисления баллов
Модуль 1, модуль 2	<p>РАБОТА НА ПРАКТИЧЕСКОМ ЗАНЯТИИ:</p> <p>Работы студентов на практическом занятии, которое состоит из трех частей: 1) устный опрос, 2) практическое задание. В случае отсутствия студента на занятии, ему предоставляется возможность отработки пропущенных занятий во время текущих консультаций. Задания для отработки аналогичны заданиям, выполняемым студентами на практических занятиях, и оцениваются по тем же критериям. Максимальное количество баллов, которые можно получить – 3 балла.</p>	<p>За каждое практическое занятие ставится от 0 до 3 баллов. Максимальная сумма баллов в семестр за данное мероприятие: 24. Оценка является совокупностью баллов за устный опрос (до 1,5 балла), выполнение практического задания (до 1,5 баллов). Оценка за устный ответ (1,5 балла) ставится во время устного опроса преподавателем студентов, за участие в обсуждении проблемных вопросов темы практического занятия, исчерпывающие ответы на вопросы преподавателя. В противном случае оценка за устный ответ не выставляется.</p> <p>Максимальный балл за практическое задание – 1,5 балла, ставится в случае выполнения всех заданий в полном объеме, грамотного их оформления (использование актуальной информации по составлению ответов на задания преподавателя; сохранение файлов с выполненными заданиями в соответствующем формате и указанной преподавателем папке).</p> <p>1,5 балла ставится в случае выполнения от 60% до 80% заданий на практическом занятии в полном объеме либо более 80% с недочетами в оформлении.</p> <p>0,75 балла ставится в случае выполнения от 40% до 60% заданий на практическом занятии в</p>

		<p>полном объеме либо более 60% с недочетами в оформлении.</p> <p>0 баллов ставится в случае выполнения менее 40% заданий, невыполнения заданий, не сохранении выполненных заданий либо не сохранении файлов в указанной преподавателем папке.</p>
<p>Модуль 1, модуль 2, модуль 3</p>	<p>АУДИТОРНАЯ КОНТРОЛЬНАЯ РАБОТА: Аудиторная контрольная работа состоит из письменной работы, компьютерного теста, двух задач. Письменная работа состоит из ответа на два теоретических вопроса, указанных в билете. Билет студент выбирает самостоятельно из предложенных преподавателем. Тест состоит из 20 тестовых вопросов.</p> <p>В случае отсутствия студента на занятии, ему предоставляется возможность отработки пропущенных занятий во время текущих консультаций (максимальное количество баллов – 26 баллов).</p> <p>При получении за контрольную работу 5 и менее баллов, студенту предоставляется возможность передачи контрольной работы (максимально возможные баллы за контрольную работу— 20 баллов).</p>	<p>Аудиторная контрольная работа оценивается в 26 баллов: письменная работа (16 баллов), компьютерный тест (4 баллов), две задачи (6 баллов).</p> <p>Каждый правильный ответ на вопрос теста оценивается в 0,2 балла (всего вопросов 20).</p> <p>Письменная работа оценивается в 16 баллов. Письменная работа состоит из ответа на два теоретических вопроса, указанных в билете. Каждый вопрос оценивается в 8 баллов.</p> <p>8-6 балла за каждый вопрос ставятся в случае: в ответе отражены определения всех понятий, указанных в билете; перечислены и раскрыты свойства и характеристики данных понятий; указаны нормативные акты, регулирующие правоотношения по поводу использования выделенных в билете объектов; дан самостоятельный творческий анализ используемых материалов. Баллы внутри критерия распределяются преподавателем самостоятельно.</p> <p>5-3 балла за каждый вопрос письменной части ставятся в случае: в ответе отражены определения всех понятий, указанных в билете; перечислены свойства и характеристики понятий; указаны нормативные акты, регулирующие правоотношения по поводу использования выделенных в билете объектов. Баллы внутри критерия распределяются преподавателем самостоятельно.</p> <p>2-1 балла за каждый вопрос письменной части ставятся в случае: в ответе отражены определения понятий, указанных в билете или свойства и характеристики понятий или указаны нормативные акты, регулирующие правоотношения по поводу использования выделенных в билете объектов. Баллы внутри критерия распределяются преподавателем самостоятельно.</p> <p>0,75 баллов за каждый вопрос письменной части</p>

		<p>ставятся в случае: в ответе отражены определения не всех понятий или отсутствуют существенные признаки, не указаны свойства и/или характеристики понятий, не указаны или указаны не верно НПА.</p> <p>0 баллов за каждый вопрос письменной части ставятся в случае полного отсутствия ответа на поставленный вопрос.</p> <p>Каждая практическая задача оценивается максимум в 3 балла. Письменное решение задачи выполняется с использованием справочных правовых систем и информационных сетевых технологий.</p> <p>3 балла за решение задачи ставится за умение правильно формулировать вопросы к решению задачи, указан ход решения (или рассуждений), использованы актуальные НПА и судебная практика, сформулированы правильные выводы.</p> <p>2 балла - правильно применены нормы права, правильно указан ход решения, но не учтены все необходимые документы.</p> <p>1 балл - за правильный выбор нормативного правового акта, но выводы сформулированы неверно.</p> <p>0 баллов – ставится, если задача не решена или решена неверно.</p>
--	--	--

ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ

Форма промежуточной аттестации	<i>зачет</i>
Формат проведения мероприятий промежуточной аттестации	<i>устно по билетам</i>
Структура мероприятий и балловая стоимость элементов	<i>1 теоретическое задание – максимально 30 баллов 1 практическое задание – максимально 20 баллов</i>

Примерные задания для мероприятий промежуточной аттестации:

Теоретические вопросы к зачету:

1. Понятие информационной безопасности и его признаки.
2. Государственная политика в области обеспечения информационной безопасности.
3. Интересы личности в информационной сфере.
4. Интересы общества и государства в информационной сфере.
5. Понятие угроз информационной безопасности. Источники угроз информационной безопасности.
6. Угрозы интересам личности в информационной сфере.
7. Угрозы интересам общества в информационной сфере.
8. Угрозы интересам государства в информационной сфере.

9. Информационное противоборство в системе угроз информационной безопасности.
10. Понятие системы информационной безопасности.
11. Силы и средства обеспечения информационной безопасности.
12. Технические средства обеспечения информационной безопасности
13. Технологические средства обеспечения информационной безопасности.
14. Организационное обеспечение информационной безопасности
15. Система государственных органов в области обеспечения информационной безопасности.
16. Правовое обеспечение информационной безопасности
17. Институт (группа институтов, подотрасль) правового обеспечения информационной безопасности в системе информационного права.
18. Содержание правового обеспечения информационной безопасности.
19. Направления правового обеспечения информационной безопасности.
20. Система правовых актов в области правового обеспечения информационной безопасности.
21. Тайна как правовая категория.
22. Общий правовой режим информации ограниченного доступа.
23. Правовой режим защиты государственной тайны.
24. Государственная тайна как особый вид информации ограниченного доступа.
25. Понятие и признаки государственной тайны.
26. Перечень сведений, составляющих государственную тайну.
27. Условия допуска к государственной тайне.
28. Доступ и допуск к государственной тайне
29. Отнесение сведений к государственной тайне и их засекречивание.
30. Ответственность за нарушение законодательства о государственной тайне.
31. Правовой режим служебной тайны.
32. Понятие служебной тайны.
33. Служебная тайна в области обороны.
34. Служебная информация ограниченного распространения в федеральных органах государственной власти.
34. Порядок работы с информацией, составляющей служебную тайну.
35. Понятие и признаки коммерческой тайны.
36. Правовой режим коммерческой тайны.
37. Группы сведений, составляющих коммерческую тайну.
38. Субъекты коммерческой тайны.
39. Условия передачи сведений, составляющих коммерческую тайну третьим лицам.
40. Понятие и признаки профессиональной тайны.
41. Правовой режим профессиональной тайны.
42. Виды профессиональных тайн.
43. Субъекты профессиональной тайны.
44. Персональные данные как форма защиты частной жизни.
45. Понятие и виды персональных данных.
46. Правовой режим обеспечения безопасности персональных данных.
47. Система законодательства о защите персональных данных.
48. Принципы и условия обработки персональных данных.
49. Обязанности оператора по обеспечению безопасности персональных данных.
50. Ответственность за нарушение законодательства о персональных данных.
51. Понятие и система информационных правонарушений.
52. Административные информационные правонарушения. Понятие и виды.
53. Дисциплинарные информационные правонарушения. Понятие и виды.
54. Гражданско-правовые информационные правонарушения. Понятие и виды.
55. Понятие и виды информационных преступлений.

Типовые практические задачи для зачета

1. Гр. Иванов заключил договор на оказание услуг хостинга с компанией Ростелеком. На размещенном в хостинге веб-сайте Иванов дал возможность всем желающим вести дискуссию и размещать материалы на тему политического устройства России.

Во время длительного отпуска Иванова на веб-сайте были размещены экстремистские материалы. Один из посетителей сайта написал об этом заявление в прокуратуру и Роскомнадзор.

Дайте правовую оценку ситуации. Как должно быть разрешено дело?

2. Гр. Иванов десять лет назад имел допуск по первой форме (особой важности) к сведениям составляющим государственную тайну и уволился из НИИ спустя 6 лет. Имея желание выехать из Российской Федерации в Великобританию он обратился в полицию с заявлением на получение загранпаспорта и разрешением на выезд. В выдаче загранпаспорта и разрешения на выезд ему было отказано. Основанием для отказа явилось заключение Межведомственной комиссии по защите государственной тайны о том, что сведения, к которым был в свое время допущен Иванов, сохраняют режим секретности. Иванов посчитал, что его права нарушены и обратился в коллегия адвокатов за юридической помощью.

О каком виде информации ограниченного доступа здесь идет речь? Дайте правовую оценку данной ситуации. Как должно быть разрешено дело?

3. Участковый уполномоченный Петровский направил в ООО «Сенко» запрос об истребовании сведений в отношении работника данной организации Заварзина. В своем запросе Петровский указал, что ему необходимо представить информацию об образовании Заварзина, его стаже работы и доходах, обоснован запрос был ссылкой на ФЗ «О полиции».

Руководитель ООО «Сенко» предоставил данную информацию Петровскому о чем стало известно Заварзину, который попросил руководителя объяснить по какой причине истребовалась данная информация и на каком основании руководитель ее предоставил. Руководитель какие-либо объяснения Заварзину давать отказался.

Заварзин обратился в суд с жалобой на действия участкового уполномоченного обосновав ее тем, что никаких преступлений и иных правонарушений он не совершал и оснований для получения его персональных данных без его согласия у участкового инспектора не было. Также Заварзин обратился в прокуратуру с просьбой привлечь руководителя ООО «Сенко» к административной ответственности.

О каком виде информации ограниченного доступа здесь идет речь? Как должно быть разрешено дело?

4. Следователь Иванов возбудил уголовное дело в отношении Васильева за отказ от дачи показаний по ст. 308 УК РФ по делу Максимова о незаконном усыновлении. По уголовному делу Васильев проходил как свидетель, а свой отказ от дачи показаний мотивировал тем, что Васильев имеет удостоверение адвоката и уже на протяжении 10 лет занимается адвокатской практикой.

Пять лет назад к нему обратился гражданин Максимов с просьбой защищать его интересы в процессе об отобрании несовершеннолетнего ребенка у своей бывшей сожительницы Петровой, а в дальнейшем лишении ее родительских прав. Васильев утверждал, что в процессе гражданского представительства ему как адвокату стали известны от гражданина Максимова сведения, которые он не имеет права и не намерен излагать суду. Как должно быть разрешено дело?

Критерии оценивания:

Билеты для зачета включают в себя 2 теоретических вопроса и 1 практическую задачу. Каждый теоретический вопрос оценивается преподавателем в 0-15 баллов, задача оценивается в 20 баллов.

Критерии начисления баллов за ответ на теоретический вопрос:

13-15 баллов ставится студенту, проявившему всесторонние и глубокие знания программного материала, освоившему в полном объеме содержание нормативно-правовых актов, изученных в течение курса, обнаружившему творческие способности в понимании и практическом использовании материала, проявившему высокие знания базовых категорий и понятий по изучаемой дисциплине. Баллы внутри критерия определяются в зависимости от количества допущенных неточностей.

9-12 баллов ставится студенту, проявившему полное знание программного материала, освоившему в полном объеме содержание нормативно-правовых актов, изученных в течение курса, обнаружившему стабильный характер знаний и умений и способному к их самостоятельному применению и обновлению в ходе практической деятельности, обнаружившему знания базовых категорий и понятий по изучаемой дисциплине. Баллы внутри критерия определяются в зависимости от количества допущенных неточностей.

5-8 баллов ставится студенту, проявившему знания основного программного материала в объеме, необходимом для предстоящей практической деятельности, знакомому с содержанием нормативно-правовых актов, изученных в течение курса, допустившему неточности при подготовке ответа, но обладающему необходимыми знаниями и умениями для их устранения при корректировке со стороны преподавателя, допустившему неточности в знаниях базовых категорий и понятий по изучаемой дисциплине. Баллы внутри критерия определяются в зависимости от количества допущенных ошибок.

1-4 балл ставится студенту, обнаружившему пробелы в знании основного программного материала, допустившему грубые ошибки при применении нормативно-правовых актов, изученных в течение курса, допустившему грубые ошибки в знаниях базовых категорий и понятий по изучаемой дисциплине. Баллы внутри критерия определяются в зависимости от количества допущенных ошибок.

0 баллов ставится студенту, который не ответил на вопрос в билете, не знает базовых категорий и понятий по изучаемой дисциплине, не знает отдельных разделов программного материала, допускает существенные ошибки, с большим затруднением отвечает на задаваемые дополнительные вопросы.

Критерии начисления баллов за решение практической задачи:

15-20 баллов за решение задачи ставится студенту за умение правильно формулировать вопросы к решению задачи, умение правильно применять нормы права и судебные акты, умение правильно решать задачу и формулировать правильный вывод. Баллы внутри критерия определяются в зависимости от количества допущенных неточностей.

8-14 баллов за умение правильно применять нормы права и правильно решать задачу. Баллы внутри критерия определяются в зависимости от количества допущенных неточностей.

1-7 балла за правильный выбор нормативного правового акта, но неправильное решение задачи. Баллы внутри критерия определяются в зависимости от количества допущенных ошибок.

0 балла – за неправильное решение задачи и неправильный выбор нормативного правового акта.

БИБЛИОГРАФИЯ ПО ДИСЦИПЛИНЕ

1. Информационные технологии в юридической деятельности: учебник для вузов / П. У. Кузнецов [и др.]; под общей редакцией П. У. Кузнецова. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-02598-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/488769>. — Режим доступа: по подписке.
2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/498844> — Режим доступа: по подписке.
3. Кузнецов, П.У. Информационное право : учебник / Кузнецов П.У. — Москва : Юстиция, 2019. — 335 с. — (для бакалавров). — ISBN 978-5-4365-2677-5. — URL: <https://book.ru/book/930199> . — Режим доступа: по подписке.
4. Фатьянов, А.А., Основные правовые системы ограничения в доступе к информации в Российской Федерации : учебник / А.А. Фатьянов. — Москва : КноРус, 2022. — 382 с. — ISBN 978-5-406-09463-1. — URL:<https://book.ru/book/943126> — Режим доступа: по подписке.
5. Дидактическая концепция цифрового профессионального образования и обучения / П. Н. Биленко, В. И. Блинов, М. В. Дулинов, Е. Ю. Есенина, А. М. Кондаков, И. С. Сергеев ; под науч. ред. В. И. Блинова – 2020. – 98 с
6. Словарь терминов и понятий цифровой дидактики / Рос. гос. проф.-пед. ун-т; авт.-сост.: Ломовцева Н. В., Заречнева К. М., Ушакова О. В., Ярина С. Ю., – Екатеринбург: РГППУ: Ажур, 2021. – 84 с.

Нормативно-правовые и правоприменительные акты:

1. Окинавская хартия глобального информационного общества (Принята на о. Окинава 22.07.2000) // Дипломатический вестник. 2000. № 8. С. 51 - 56.
2. Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Российская газета, N 25, 13.02.2009,
3. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» // Российская газета, № 168, 30.07.2010,
4. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Российская газета, № 75, 08.04.2011,
5. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ 05.12.2016 № 646) // "Собрание законодательства РФ", 12.12.2016, № 50, ст. 7074
6. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы (утв. Указом Президента РФ 09.05.2017 № 203) // "Собрание законодательства РФ", 15.05.2017, № 20, ст. 2901
7. Постановление Правительства РФ от 28.01.2002 № 65 «О федеральной целевой программе "Электронная Россия (2002 - 2010 годы)"» // СЗРФ, 04.02.2002, № 5, ст. 531,
8. Постановление Правительства РФ от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия» // СЗРФ, 20.09.2010, № 38, ст. 4823.

9. Распоряжение Правительства РФ от 20.10.2010 № 1815-р «О государственной программе Российской Федерации "Информационное общество (2011 - 2020 годы)"» // СЗРФ, 15.11.2010, № 46, ст. 6026.
10. Распоряжение Правительства РФ от 27.09.2004 № 1244-р «О Концепции использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года и плане мероприятий по ее реализации» // СЗРФ, 04.10.2004, N 40, ст. 3981,
11. Распоряжение Правительства РФ от 17.07.2006 № 1024-р «О Концепции региональной информатизации до 2010 года» // СЗРФ, 24.07.2006, № 30, ст. 3419.
12. Распоряжение Правительства РФ от 06.05.2008 № 632-р «О Концепции формирования в Российской Федерации электронного правительства до 2010 года» // СЗРФ, 19.05.2008, № 20, ст. 2372.
13. Указ Президента РФ от 10.10.2019 N 490 «О развитии искусственного интеллекта в Российской Федерации»
14. «Методические рекомендации по цифровой трансформации государственных корпораций и компаний с государственным участием» (утв. Минцифры России) 02.04.2021
15. «Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019 - 2021 годов» (утв. Банком России) 28.09.2020
16. Распоряжение Правительства РФ от 22.10.2021 N 2998-р «Об утверждении стратегического направления в области цифровой трансформации государственного управления»
17. Приказ Генеральной прокуратуры РФ от 14 сентября 2017 г. № 627 «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года»

Сквозные технологии в юриспруденции

1. Искусственный интеллект в области юриспруденции: [Электронный ресурс]. URL: <https://habr.com/ru/post/506086/>
2. Искусственный интеллект в области юриспруденции. Статья 2: [Электронный ресурс]. URL: <https://habr.com/ru/post/511004/>
3. Искусственный интеллект в области юриспруденции. Статья 3: [Электронный ресурс]. <https://habr.com/ru/post/515510/>
4. Искусственный интеллект в области юриспруденции. Часть 4: [Электронный ресурс]. <https://habr.com/ru/post/523126/>
5. Электронное правосудие. Электронный документооборот : научно-практическое пособие / В. А. Лаптев, Н. И. Соловяненко ; под общ. ред. С. Ю. Чучи. – Москва : Проспект, 2021. – 240 с. - ISBN 978-5-392-34436-9 ; [Электронный ресурс]. - URL: <http://ebs.prospekt.org/book/37387>
6. Синкевич, К. В. К вопросу о влиянии искусственного интеллекта на юридическую профессию в цифровую эпоху: // Журнал Белорусского государственного университета. Право, 2021. 3. 45-54. URL: <https://journals.bsu.by/index.php/law/article/view/4171>

Перечень электронных учебных изданий

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/498844>. — Режим доступа: по подписке.

2. Кузнецов, П.У. Информационное право : учебник / Кузнецов П.У. — Москва : Юстиция, 2019. — 335 с. — (для бакалавров). — ISBN 978-5-4365-2677-5. — URL: <https://book.ru/book/930199> . — Режим доступа: по подписке.
3. Фатьянов, А.А., Основные правовые системы ограничения в доступе к информации в Российской Федерации : учебник / А.А. Фатьянов. — Москва : КноРус, 2022. — 382 с. — ISBN 978-5-406-09463-1. — URL:<https://book.ru/book/943126> — Режим доступа: по подписке.
4. Информационные технологии в юридической деятельности: учебник для вузов / П. У. Кузнецов [и др.]; под общей редакцией П. У. Кузнецова. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-02598-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/488769>. — Режим доступа: по подписке.
5. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: <https://doi.org/10.29039/1761-6176>.
6. - ISBN 978-5-369-01761-6. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1861657>. - Режим доступа: по подписке.

Электронные учебные издания доступны для зарегистрированных в Электронной информационно-образовательной среде университета пользователей

Оснащение помещений для учебных занятий

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебная аудитория для проведения занятий лекционного типа	Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: рабочие места для обучающихся, рабочее место преподавателя, экран проекционный, проектор, доска магнитно-меловая, учебно-наглядные пособия, обеспечивающие тематические иллюстрации, видеонаблюдение
Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Специализированная мебель и технические средства обучения, служащие для представления учебной информации большой аудитории: рабочие места для обучающихся, рабочее место преподавателя, доска магнитно-меловая, учебно-наглядные пособия, обеспечивающие тематические иллюстрации, моноблок, интерактивная доска
Помещение для самостоятельной работы	Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду

	организации, проектор, экран, многофункциональное устройство
--	--

Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. Microsoft WINEDUperDVC ALNG UpgrdSAPk OLV E 1Y AcademicEdition Enterprise;
2. Linux (Альт, Астра);
3. Kaspersky Endpoint Security 11 для Windows;
4. Libre Office (свободно распространяемое программное обеспечение).

Перечень электронно-библиотечных систем:

1. «Электронно-библиотечная система ZNANIUM»;
2. «Образовательная платформа ЮРАЙТ»;
3. Электронно-библиотечная система «BOOK.ru»;
4. Электронно-библиотечная система «ЛАНЬ»;
5. Электронно-библиотечная система Издательства «Перспект».

Перечень современных профессиональных баз данных

1. Электронная библиотека диссертаций (ЭБД);
2. Единая межведомственная информационно – статистическая система (ЕМИСС) - Режим доступа: <https://fedstat.ru/>;
3. База данных показателей муниципальных образований - Режим доступа: <https://rosstat.gov.ru/storage/mediabank/Munst.htm>;
4. ПРЕДОСТАВЛЕНИЕ СВЕДЕНИЙ ИЗ ЕГРЮЛ/ЕГРИП В ЭЛЕКТРОННОМ ВИДЕ - Режим доступа: <https://egrul.nalog.ru/index.html>;
5. Государственная автоматизированная система Российской Федерации «Правосудие» - Режим доступа: <https://bsr.sudrf.ru/bigs/portal.html>;
6. Банк решений арбитражных судов - Режим доступа: <https://ras.arbitr.ru/>;
7. База данных судебных актов - Режим доступа: <http://bdsa.minjust.ru/>;
8. База решений и правовых актов Федеральной антимонопольной службы - Режим доступа: <https://br.fas.gov.ru/>;
9. Банк решений Конституционного Суда Российской Федерации - Режим доступа: <http://www.ksrf.ru/ru/Decision/Pages/default.aspx>;
10. Государственная система правовой информации – Режим доступа: <http://www.pravo.gov.ru/>;
11. Федеральный портал проектов нормативных актов - Режим доступа: <https://regulation.gov.ru/>;
12. Система обеспечения законодательной деятельности - Режим доступа: <https://sozd.duma.gov.ru/>.

Перечень информационных справочных систем

1. Информационно-правовой портал «Система Гарант»;
2. Справочная правовая система «КонсультантПлюс»;
3. Информационно-правовая система «Кодекс»;
4. Информационно-правовая система (ИПС) «Законодательство стран СНГ».